EXHIBIT 5

Freedom to Tinker

… is your freedom to understand, discuss, repair, and modify the technological devices you own.

« DRM, Incompatibility, and Market Power: A Visit to the Sausage Factory
Not Just Another Buggy Program »

MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug

Wednesday December 7, 2005 by Ed Felten

iSEC, EFF, and SonyBMG issued a joint press release yesterday, announcing yet another serious security bug in the SunnComm MediaMax copy protection software that ships on many SonyBMG compact discs. (SonyBMG has recalled CDs that use another copy protection system, XCP, but they have not yet recalled discs containing MediaMax.)

As we've written before, the first time you insert a MediaMax-bearing CD into your Windows computer (assuming you have Windows autorun enabled, as most people do), MediaMax installs some software on your computer. Once this initial software is on your computer, you are vulnerable to the new attack. The gist of the problem is that MediaMax installs itself in a directory that anyone is allowed to modify, even users who otherwise run with heavily restricted security permissions. Any program that comes along can modify your MediaMax files, booby-trapping the files by inserting hostile software that will be run automatically the next time you insert a MediaMax-bearing CD into your computer. And because MediaMax is run with full administrator privileges, the hostile program gets to run with full privileges, allowing it to inflict any mischief it likes on your PC.

Alex Halderman has discovered that the problem is worse than the press release indicates:

- You are vulnerable **even if you decline the MediaMax license agreement**. Simply inserting a MediaMax-bearing CD into your PC paves the way for an attacker to come along and set a booby-trap. The trap will be sprung the next time you insert such a disc.
- SonyBMG has released a patch that purports to fix the problem. However, our tests show that **the patch is insecure**. It turns out that there is a way an adversary can booby-trap the MediaMax files so that hostile software is run automatically *when you install and run the MediaMax patch*.
- **The previously released MediaMax uninstaller is also insecure** in the same way, allowing an adversary to booby-trap files so that hostile software is run automatically when you try to use the uninstaller.

  (These attacks are similar to the exploit described in iSEC's report, but they involve a different modification to the MediaMax files.)

Because of these problems, we recommend for now that if you have a Windows PC, you (1) do not use the MediaMax patch, (2) do not use the previously released MediaMax uninstaller, and (3) do not insert a MediaMax-bearing CD into your PC.

We have notified SonyBMG and MediaMax about these problems. We assume they will develop a new uninstaller that safely rids users' computers of the MediaMax software once and for all.

The consequences of this problem are just as bad as those of the XCP rootkit whose discovery by Mark Russinovich started SonyBMG's woes. This problem, like the rootkit, allows any program on the system to launch a serious security attack that would normally be available only to fully trusted programs.

According to the press release, SonyBMG intends to use MediaMax's banner ad display feature to warn users about these vulnerabilities. While this is a positive step, it will fail to reach users who have rejected the MediaMax license agreement. This group is at particularly high risk, since they are probably unaware that the software is installed on their computers.

Worst of all, it is impossible to patch the millions of MediaMax-bearing CDs that are already out there. Every disc sitting on somebody's shelf, or in a record-store bin, is just waiting to install the vulnerable software on the next PC it is inserted into. The only sure way to address this risk is take the discs out of circulation.

The time has come for SonyBMG to recall all MediaMax CDs.

UPDATE (Dec. 9): Sony and MediaMax have issued a new patch. According to our limited testing, this patch does not suffer from the security problem described above. They have also issued a new uninstaller, which we are still testing. We'll update this entry again when we have more results on the uninstaller.

This entry was posted on Wednesday December 7, 2005 at 10:33 am and is filed under Security, DRM, Privacy, CD Copy Protection. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

Ubeatable Copy Protection
Alan Technology Technology for Software & Hardware

Digital Video Stabilizer
Removes copy protection from videotapes. Low price.

Ads by Goooooogle

Advertise on this site

66 Responses to "MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug"

1. *Avery J. Parker - Web site hosting and computer service* Says:
   December 7th, 2005 at 11:01 am

   […] Once more in the continuing story…. According to freedom-to-tinker, the "fix" released today for the SunnComm/Mediamax DRM software (the "other" DRM software on sony/bmg discs). Is fatally flawed. The problem the software initially poses is much worse than the company lets on in their release and their advise is…. 1) don't play a mediamax protected disc in your pc. 2)don't use the fix, 3) don't use the old uninstaller. […]

2. *Eddie hates copy protection* Says:
   December 7th, 2005 at 11:29 am

   I'll have to hand it to you Eddie and Alex, you certainly have a penchant to deride Mediamax and an obvious distaste for any kind of audio copy protection in the market place. What are your feelings on game, software and DVD copy protection? Do you feel it is your right to copy those as well?

3. *JayCee* Says:
   December 7th, 2005 at 11:51 am

   The list of cd's that MediaMax is oddly only on the "BMG" side of the company's releases- I think it's something like RCA and Jive Records. Any info online from those labels? (example: rcarecords.com)

   I noticed that the labels formerly only under Sony have big fat links to XCP info on their sites (like columbiarecords.com)…

4. *AB* Says:
   December 7th, 2005 at 11:52 am

   Here's the reply I received from their tech support when I said their ActiveX utility was problematic. If you reboot, does it remove the threat?

   "Unfortunately, this is the only means by which to uninstall MediaMax. However, as previously noted, the Active X control installed is removed upon your next reboot. It will list all files left on the system as they are system files only shared by MediaMax. There is no security risk involved with this removal process. Due to recent media involving problems with other copy protection softwares, our utility has been tested extensively, both interneally and externally, and there is zero security risk. If you wish to uninstall MediaMax from your system, you must use this utility."

5. *I hate trolls* Says:
December 7th, 2005 at 11:52 am

Do you feel it is your right to post to a blog when you likely work for the companies that thrust this anti-consumer grbage on us?

"Do you feel it is your right to copy these as well?"

Please.

All people want is the ability to play music on the CD-Players INSIDE THEIR COMPUTERS without it opening gaping holes in the secuirty of Windows. If people copy them, that's their business, but I should be able to play a few songs at work without causing massive security problems on a machine, and have a compnay that doen't lie and procrastinate around the issue to save a little money.

6. *Eddie hates conspiracy theorists* Says:
December 7th, 2005 at 12:32 pm

Now there was an educated response to a genuine question. Got anymore ammo in that artillery box of a non sequitur?

7. *Mike* Says:
December 7th, 2005 at 12:36 pm

Unbelivable. Some companies dig their own graves, some use a backhoe. Sony is apparently trying for First Place in the latter category. Sony has become the Bad News Buffet.

Mike
http://www.quicktrivia.com

8. *Mike* Says:
December 7th, 2005 at 12:44 pm

'Eddie hates copy protection' wrote: "I'll have to hand it to you Eddie and Alex, you certainly have a penchant to deride Mediamax and an obvious distaste for any kind of audio copy protection in the market place."

Duh. What was your first clue? Did ya ever wonder why we feel that way?

I mean, reall- is it too much to ask that the products we spend our money on don't infect or destroy our PCs, or leave it vulnerable to exploit code? Gee, that's SOOOOO unreasonable.

Mike
http://www.quicktrivia.com

9. *I hate MediaMax investors* Says:
December 7th, 2005 at 12:49 pm

Give it a rest, Eddie H (or are you really Steve K).

MediaMax installs a privilege escalation vulnerability as soon as the user inserts the CD. Before even displaying the EULA. That deserves a recall.

Also, the fact that the vulnerable software adds absolutely no value to the user's experience (and in fact destroys value by preventing the user from using the CD with his software or portable music player of choice) leaves a bad taste in the mouth of anyone who isn't a MexiaMax employee or shill.

10. *tRellium* Says:
December 7th, 2005 at 1:29 pm

I don't mind buying my music, I don't mind copy protection. I absolutely hate when it completely obliterates my security systems which already suffer a heavy enough birage from hackers. I don't see why Sony should join their cause in this.

I am against the security defects, and that they are implemented on purpose, and that the EULA is designed to force me to accept all further impositions on my property on Sony's whim without any further need to tell me whats going on in my own computer.

What I seek is a simple system that is hard to implement. Let me buy my music LEGALLY from a website (ie iTunes) and let me get digital versions encrypted for all my playing devices … which are also legally bought. Let me decide if I listen to the music on my computer, home theater, car, or portable player. I payed for it, and I want to pay more in the future for more of that.

What I don't want is music systems that force security breaches, and also limit where I can possibly play music I purchased, and restricts where that music might be played in the future (such as Windows Vista, which isn't supported by the currently shipped disks).

It has nothing to do with copying the music. That has been done for 50+ years. We always could copy a record to tape and listen to it in the car, even in the 1970's.

I want reasons to buy more music, not reasons to avoid it at all costs. I also don't like that Sony makes it SO obvious that its safer to download the pirated mp3's than to use their system of "protection". Their "protection" is at odds with mine. The only winners are the pirates.

Sony is their own worst enemy. If they really wanted to make a profit on this, they should take the music off the disks, and sell their root kit technology to the pirates for $50 a disk. Why is it that this actually makes sense, and I suspect teh pirates would be all for it?

Lets face it, comments made by "Eddie hates copy protection" above could indicate a person on Sony payroll, or someone who wants further security holes created to force in their own malware. The hackers don't want the disks removed from the marketplace, they want them inserted into every computer. So does Sony.

11. *Anonymous* Says:
December 7th, 2005 at 2:46 pm

NGS Director Robert Horton said, "After carefully researching the security vulnerability presented to us by SONY BMG, we have determined that it is not uncommon and, importantly, it is easily fixed by applying a software update."

12. *Anonymous* Says:
December 7th, 2005 at 2:48 pm

NGS lead the world in enterprise level application vulnerability research and database security, the delivery of sophisticated security software and expert consulting services. The NGS team include internationally renowned security researchers and more CHECK Team leaders than any other UK security organisation. NGS are based in the United Kingdom, but provide our services and unique skills set to some of the largest and most demanding organisations around the globe. NGS have published more advisories regarding high level enterprise application vulnerabilities than any other security company. NGS are a trusted computer security provider for some of the largest companies in the world, why not see what we can do for you?

13. *Anonymous* Says:
December 7th, 2005 at 2:53 pm

"not uncommon and, importantly, it is easily fixed by applying a software update"

14. *Bill McGonigle* Says:
December 7th, 2005 at 3:00 pm

Digital media isn't very interesting if you can't copy it, Eddie H. If I'm playing a CD in my computer's drive out to my speakers on a USB DAC, it's probably being copied a half dozen times between media, IC's and memory locations. And precisely _because_ I can do this, I buy CD's. There is a direct cause and effect relationship here. If I can't do this I won't buy the CD, plain and simple. If you want to make it hard to copy music, I recommend wax cylinders or roving minstrals.

15. *TomCS* Says:
December 7th, 2005 at 3:32 pm

I've thought from the beginning that the real threat to user (and PC copying fair use) rights was Sunncomm, which was at least a half competent implementation, and not XCP. MediaMax is apparently on about 250 discs, most not SonyBMG products. (I even suspected that XCP might be an intentional mistake, to allow Sunncomm and MediaMax to sneak in as "acceptable" DRM; but that is black helicopter stuff, surely.)

So what to do about SonyBMG, and the others that use Mediamax or XCP?

If Sony is too remote, let's tackle our local rootkit and spy ware distributors. Let's ask our local record store either to withdraw all these discs, or at least move them to separate racks, so people who think they are buying a compliant CD don't get a bad surprise when they get home. And let's ask our local consumer law advocates to think about class action suits against the retailers.

16. *V* Says:
December 7th, 2005 at 3:56 pm

Eddie, I'm against all forms of DRM as well and I don't consider this a radical view. I want open standards (such as the audio CD that has made companies like SonyBMG a fortune) and the MP3. I want content that does not try to protect itself from the people who paid for it, especially when it causes a security issue.

I don't think this is an unreasonable request, especially since it's a well known fact that DRM doesn't work. The industry calls it a "speed bump," and, like real speed bumps, anyone who choose to cross it will have no difficulty doing so:

I have a friend who has a very good sized DVD collection. He's spent hundreds of dollars on this content, which he legally owns. He believes that he's entitled to make copies of his DVDs for personal use, so long as he doesn't distribute them. He uses a program called DVDShrink, which is no more inconvenient than holding down the shift key, or even burning a copy of unencoded content.

17. *The PC Doctor* Says:
December 7th, 2005 at 5:03 pm

More bad news for Sony/SunnComm

Geez, more bad news for Sony and SunnComm …
Today SunnComm released a patch for a security vulnerability in their MediaMax DRM software … problem is, the update suffers from the same security bug.
Question - are there any decent program…

18. *Eddie is not ready...to dump stock* Says:
December 7th, 2005 at 7:21 pm

Guys, "Eddie Hates…"/Anonymous is just another SunnComm stockholder or insider. Sony felt like they could

take (or had to take) the hit with the rootkit, but MediaMax is on ten times more CDs and a recall right now would be a disaster for holiday sales. Not to mention what it would do to SunnComm stock. Right, Eddie?

19. *April Newton* Says:
December 7th, 2005 at 9:14 pm

SunnComm's latest comment on new patch error discoverers.

Today, from SunnComm investor relations consultant Mario "IKE" Iacoviello. What can one expect from a company that hires him as IR consultant.

"Felton and Halderman seem to be subjectively against, copy-protection.
They are subjectively against our fix, no one else including the EFF is complaining about the "fix". We will however fix the "fix" just for EVERYONES satisfaction. This is being done in real time. We will be successful!!! sony/bmg is committed to US and copy-protection. This too shall pass and we will be standing. We will not die only get stronger with every step. "

http://www.investorshub.com/boards/read_msg.asp?message_id=8782969

What the SEC had to say about Mario "IKE" Iacoviello

http://www.sec.gov/litigation/admin/34-41940.htm

How Mario defines his position in SunnComm

http://www.investorshub.com/boards/read_msg.asp?message_id=8335846

20. *pissed off as hell* Says:
December 7th, 2005 at 10:55 pm

what everyone either dose not realise or wont say is that sony/bmg/suncom/mediamax/ who ever didnt write bad and usecure software by accident they wrote is intentionaly they want a back door into everyones PC so they can scan,document,controle and if need be prosecute users or delet users MP3's regardless of how they got them.

think of all thee back doors as a test case just put them in and do nothing for now then later on if they dont get caught slowley start adding sub7 like trojens and things of this nature to scan a users PC for whatever they deem is copy infingment and either delete it ir copy a users info AND files to use to prosecute. i really cant see how much more sinister these music companys can get.

think about it all these "securety flaws" from a company as huge as sony? a company thats been in the software and hardware bisiness for how many years can not be that incompitent. it MUST be intentional

21. *hello_world* Says:
December 7th, 2005 at 11:22 pm

A CD is a a CD per the Philips spec of old http://www.licensing.philips.com/information/cd/audio/. The CD predated the PC.

The sellers and distrubutors should be held liable for selling a mislabled product. A Red-book CD should not be sold as a Blue-book CD.

A mixed content CD with binaries is not a "CD". A non-compliant "CD" should not be mixed in with regular CD's on the store shelf.

IF Sony etc wants to sell music which does not have the "problem" with ripping, distrubuting etc, I suggest they use another format.

22. *Taz* Says:
December 8th, 2005 at 1:49 am

I have to agree with V… "(such as the audio CD that has made companies like SonyBMG a fortune)".

As technology progresses the cost of the technology should go down. The Audio CD has been out for decades and these days anyone with a computer/mic/and some software can create, mix and burn their own Audio CD. This fact alone should have brought the price of an Audio CD down in price. I can buy a feature movie on DVD for less than an Audio CD these days.

I think that any kind of DRM or copy protection on any kind of digital media is stupid. All it does is create a whole other market for things to circumvent the copy protection, for example the mod chips for the PS2 and orig Xbox… and I am sure that there are already people hacking and cracking the Xbox 360 and they will make and manufacture and sell stuff to circumvent its DRM's etc.

23. *Mike Birney* Says:
December 8th, 2005 at 3:13 am

I agree with "pissed off as hell Says". The plan all along was to get MediaMax on to as many PCs as possible, by hook or by crook. This is a comment from Peter Jacobs in a CNET article from 2 years ago.

"Future versions of the SunnComm software would include ways that the copy-protecting files would change their name on different computers, making them harder to find, Jacobs said. Moreover, the company will distribute the technology along with third-party software, so that it doesn't always come off a protected CD, he added."

http://news.com.com/2100-1025-5089168.html

That's why the Shift Key issue was no big deal to Sony-BMG. Even though the typical non-techical user (probably 95% of users) might be aware of the Shift Key bypass, they only had to forget to press it once playing any MediaMax CD to ensure that the the driver was loaded. We know from Ed's and Alex's excellent investigations, that if the user forgot to press the Shift Key, then declining the EULA that would then come up would not stop the driver being loaded. That was no bug, but completely intentional. Although the non-techical user might be aware of the shift key, they would be out of their depth trying to remove the driver once installed. That's why there was no uninstaller made widely available until recently and then only after this whole debacle blew up in their faces. The uninstaller is also only on request and not included with the CD software.

Even Sonopress, BMG's manufacturing arm, was in on the act. They signed an agreement to market MediaMax to the other labels, including BMGs competitors.

"Sonopress is already producing commercial and promotional CD releases in North America utilizing the MediaMax technology and is ready to aggressively market and deploy this music management product on a global basis."

http://www.sunncomm.com/press/pressrelease.asp?prid=200312090900

If you believed your product was superior, why market it to your competitors. The reason was the mutual advantage they would all gain by having as many PCs infected as quickly as possible.

You even had ludicrous claims of the products effectiveness.

"After the first week, sales of the Hamilton CD dropped 23 percent, to 25,598 copies, according to Nielsen SoundScan, which tracks music sales. The typical first-week drop-off is 40 to 60 percent, said Jordan Katz, senior vice president of sales at Arista."

http://www.investorshub.com/boards/read_msg.asp?message_id=8779089

But notice the out clause a bit further down.

"I know my science well enough to know that correlation does not mean causation," Katz said. "I would not go out on a limb and say this was the only reason [sales] were down only 23 percent. However, I would say it was a contributing factor."

He forgot to mention the other contributing factor, which was the massive promotion given to that CD. This was all to impress other labels and hope they would join in.

Even though the casual user could use the Shift Key to bypass the copy protection, if they didn't it still allowed them to make up to 3 copies. In fact it was easier for the casual user to make 3 copies using MediaMax than without it, as it provided a single click implementation, compared to using other burning software. But to make matters worse, the 3 copies that MediaMax allowed you to make, were each unprotected, so using those as the source allowed a further unlimited number of copies to be made. So any suggestion that it was the effectiveness of the copy protection that caused the reduced drop off is illogical. It was the massive promotion that was responsible.

The plan was that over time a significant percentage of PCs would have been infected with the driver (even through sources other than music CDs as per Jacob's comment) and the labels could then tighten the screws by changing some of the parameters (number of copies allowed, etc.). They would also have the DMCA to back them up if 3rd party uninstallers were made available, as it is illegal under the DMCA to try and circumvent copy protection s/w.

Sony-BMG went to bed with SunnComm even though they were aware that the company was scandal ridden, as many have shown in various posts. That in fact suited them, as it provide several additional reasons to drop SunnComm if their plan went awry.

We should be forever thankful for Ed and Alex discovering the underhand side of MediaMax protection; the install without permission and the spyware aspect.

A total recall of all MediaMax CDs should be demanded. Existing problems should be fixed and an uninstaller should be included before MediaMax is put back on the market.

24. *"New security flaw vexes Sony BMG piracy battle"* Says:
December 8th, 2005 at 3:38 am

"New security flaw vexes Sony BMG piracy battle"

http://www.boston.com/business/technology/articles/2005/12/08/new_security_flaw_vexes_sony_bmg_piracy_ba

"But yesterday, Halderman struck again. He said that Sony BMG's patch was also flawed and could actually cause the security problem it was supposed to block."

25. *Mike Birney* Says:
December 8th, 2005 at 6:03 am

"SONY BMG will notify consumers about this vulnerability and the update through the banner functionality included on the player"

Of course that implies that MediaMax goes to the Sony-BMG website whenever you play the CD or the downloaded music. More proof its spyware.

26. *Computerworld Blogs* Says:
December 8th, 2005 at 7:09 am

Gartner yells whoah, Yahoo! copies! Skype! (and =A1+snare)

In today's IT Blogwatch, we stare like a sullen teenager at Gartner's advice to would-be BlackBerry users. Also Yahoo! does a Skype. Not to mention a drum machine running in Excel…

27. *Tim Thomas* Says:
December 8th, 2005 at 8:11 am

As long as I have tape-monitor jacks on my home stereo amp and a stereo line-in jack on my sound card, there will never be copy protection. All this DRM crap in moronic, at best. Sampling analog signals is real-time, and therefore seems slow compared to ripping. However, when you consider the fact that I do it when I listen to the CD anyway, you realize my incremental time to digitize tracks is actually quite small. "There is no security."

28. *Hooper3* Says:
December 8th, 2005 at 11:03 am

"The time has come for SonyBMG to recall all MediaMax CDs."

I agree completely, but as of December 6th, my local Walmart was still stocking and selling XCP infected cd's.

29. *Colin* Says:
December 8th, 2005 at 11:35 am

I have for some refused to buy anything from Sony. Two reasons - one wherever possible they make proprietary stuff forcing me to buy from Sony & two apart from the intial product everything to do with Sony organisation is shit. Now I have another - invasion of my privacy like a thief in the night

30. *Mark Christiansen* Says:
December 8th, 2005 at 1:25 pm

Perhaps I should not feed the troll but here goes…

Having bought my copy of music, software, video, literature or any other such thing I do expect to copy it. I expect to make backups or translate to another format or use from another machine or use it pretty much any way I please and to sell it when I am done using it. What I don't expect to do is make copies for other people or keep any of the backups or translations I made once I sold the copy I bought or give public displays which compete with the copyright owner's ability to sell the thing in the market.

Copyright maximalists want every little use to be subject to permission. This is so the market can be subdivided and prices optimized with every dollar extracted from buyers. It is also a legal dodge to turn the given monopoly over a specific creative work into an effective monopoly over other things not covered by law.

Copyright is not a right of authorship but instead a bargain. Fair, working bargains have two sides where both parties come out ahead. Such balance is long gone from copyright as we have today. Where is the publics benefit in this bargain where we pay for government enforcement with penalties far out of reasonable proportion, tolerate digital restrictions management and give effectively permanent duration?

Laws which give practical approximations to justice and fairness get a lot of respect and deserve more. Laws which reflect power and its abuse get little and deserve less.

31. *tRellium* Says:
December 8th, 2005 at 3:37 pm

Sony is a big company. If they really wanted to they could design a complex encryptions system, and embed that in every walkman they sell, every stereo they manufacture, and every computer they assemble. Then they could encrypt each song specifically for one person to use on each of those devices, and freely make backup copies from.

The problem is that the total number of people who want to only buy Sony products to listen to only Sony media is probably too limited to be worth going to all this fuss.

But, they do have a choice to go that road in order to minimize the threat of piracy.

Instead, to bolster sales, Sony wants to use an open and standard medium on which songs can be played easily but which has the down side of being easy to duplicate, and difficult to lcoate the people who distribute freely. That's the price they pay, and its the system in place, and its Sony's choice to enter the market under those conditions.

What they want to do is access that powerful market, but protect themselves as if its a private meeting of close friends. It won't work. They should pick a system, they are big enough to invent their own.

I don't trust that they aren't trying to curb the usefulness of current generation CD's so that we need to buy them again in a few years. They complain an awful lot about piracy, but they also don't mention that I own 3 or more versions of some music (two records, tape, and CD versions). All those were purchased, they got paid at least 3 times by me for that one product.

Sony does have a choice about how they market their intellectual property, and I have the choice whether I want to buy in to it … as long as they tell me HONESTLY about how they operate.

32. *Saskboy* Says:
December 9th, 2005 at 8:18 am

Sony is going to have to recall the CDs now. This is fantastic, since it might finally get the message out that all DRM is bad and breaks computers.

Sony shouldn't have got into the business of modifying people's computers unless they are willing to take on the task of computer security.

http://www.boycottsony.us ought to have a ball with this news.

I found this page through Slashdot.org

33. *Anonymous* Says:
December 9th, 2005 at 11:20 am

"It's a fairly common issue often found in PC games," said Robert Horton, a security expert from NGS Software brought in by Sony to vet its latest patch.

"Its fairly common and the fix is easy to provide through a software update."

He said it was unlikely that any attacker would have been able to exploit the bugs in MediaMax and its patch.

34. *Anonymous* Says:
December 9th, 2005 at 1:33 pm

UPDATE (Dec. 9): Sony and MediaMax have issued a new patch. According to our limited testing, this patch does not suffer from the security problem described above. They have also issued a new uninstaller, which we are still testing. We'll update this entry again when we have more results on the uninstaller.

35. *Anonymous* Says:
December 9th, 2005 at 4:05 pm

MediaMax CEO, Kevin Clement, Comments on Recent Events

"I am incredibly excited to be here at MediaMax Technology. MediaMax and SunnComm are two fantastic organizations defined by talented and dedicated team members. These organizations have consistently delivered solid, tested and certified technology solutions for years," comments Kevin Clement, MediaMax's recently appointed and on-the-job president and CEO. "I intend to develop a world-class technology organization focused on delivering high-quality, secure, consumer friendly content protection solutions.

I have been working closely with our record label customers, security firms and other industry groups to ensure that we are addressing any and all concerns regarding our industry-leading MediaMax product. Recently, our software has come under intense scrutiny from the technical community following a series of accusations relating to security issues and code infringement against one of our competitor's products. We take all potential security issues very seriously. As such, our teams respond immediately upon notification of any potential security vulnerability."

SunnComm is a software company. Software companies routinely issue patches and updates. This is not uncommon and is an accepted practice. Due to the structure of current operating systems, we all are constantly reminded of the need to upgrade software for various reasons. This process applies to software that we use every day including media players, browsers, word processors and even the operating systems themselves. The reality is that we will be called upon from time to time to issue patches and updates to our software. We understand and accept this responsibility. We always strive to deliver well designed code that is 100% bug free and provides secure solutions. As history has shown, this is not always possible to do, even for the largest software companies.

The true worth of a software company is not how perfect their code is, it can never be perfect, but rather how quickly they respond to valid concerns regarding the security and stability of their product and more importantly, how quickly and efficiently they deliver a solution. MediaMax Technology takes potential security vulnerabilities very seriously. This will never change. Recent news events along with an increased level of scrutiny have created challenges for our entire industry. MediaMax Technology, along with our strategic partner, SunnComm International, has responded quickly and with decisiveness. SunnComm has consistently worked with its partners and multiple software security firms in order to thoroughly test and ultimately deliver completed secure resolutions. We have delivered these in a timeframe of days where the norm in the software industry is to respond within a month. We will always strive to deliver corrective solutions in a period of time that exceeds the expectations of our customers and their consumers.

There are very vocal groups and individuals who do not believe in the use of DRM technology. This is a philosophical debate that will not be settled anytime soon. MediaMax Technology's responsibility is to deliver content protection solutions that balance protecting the intellectual property owner's rights and the expectations of their consumers. We are focused on delivering high-quality, secure, consumer friendly content protection solutions.

Kevin concludes, "Our software solutions are being improved every day. You have my word that we will not stop working to make our products better, more secure, more consumer friendly and more valuable to our customers. As we emerge from this period of intense scrutiny, our solutions and, more importantly, our company will be better because of it. I would like to point out that no other CD or DVD copy protection technology has ever undergone the type of intense scrutiny that MediaMax has encountered. The development team has addressed every valid issue that has been presented and has made the necessary adjustments. The current MediaMax product is now the most secure, tested and scrutinized copy protection technology available anywhere in the world. We intend to immediately begin leveraging this incredibly stable, well-tested core technology in our plans to develop and deploy new content protection solutions in new markets and industries. Our mission is clear - develop a world-class technology organization focused on delivering high-quality, secure, consumer-friendly content protection solutions. These recent events have served to make us battle tested and better then ever."

36. *Anonymous* Says:
December 9th, 2005 at 10:55 pm

Ed, this statement should be officially retracted along with a letter of apology…

"another serious security bug in the SunnComm MediaMax copy protection software"

According to the security experts…

"It's a fairly common issue often found in PC games," said Robert Horton, a security expert from NGS Software brought in by Sony to vet its latest patch.

"Its fairly common and the fix is easy to provide through a software update."

He said it was unlikely that any attacker would have been able to exploit the bugs in MediaMax and its patch. "

Just because you obviously have little experience with this type of software flaw, does not entitle you to use these inflammatory statements. (If you do have experience with these common issues that are easily fixed, then why are you characterizing them in a different light?) According to the experts, there never was a 'serious security flaw' with this issue.

I anxiously await your retractions, corrections and apologies.

37. *Attempting a rational thoght* Says:
December 10th, 2005 at 12:30 am

If Sony BMG is so paranoid about potential copyright infringement of its musical properties, why don't they just take the logical step and stop producing music? Think about it: No music means no having to produce media that must be, in their minds, protected by fatally flawed software, no worrying about how "pirates" might crack DRM and copy songs, no having to deal with negative media attention once it's obvious that their product can bring about operating-system level destruction and leaves users vulnerable to malicious attacks. And no having to pay performers royalties or other payments, no having to foster new musical acts, no having to compete against competitors, no having to pay for the costs of recording, manufacturing, and packaging media, no having to spend money on marketing campaigns and radio promotions (although the recent payola scandal at Sony BMG is another stoy entirely), not having to pay software companies for writing and maintaining DRM schemes, no having to search out new companies and new DRM schmes to stay one step ahead of "pirates", no corporate expenditures at all on music. It'll save Sony BMG a bundle, prevent "pirates" from negatively impacting the bottom line (how can music be pirated if it's never heard?), and spare Sony BMG from poor album sales! How can Sony BMG fail to see this is the only logical solution to their piracy problems? Sony BMG, for the good of your bottom line and yearly profit statement, stop producing music now.

Realistically, though, Sony BMG (and the recording industry in general) would probably try to have the stereo jacks that allow headsets to be attached to stereos, microphones to be attached to computers, etc., and the RCA stereo cables one can use to establish connections between a cassette player and computer, cassette player and stereo system, etc., outlawed before ceasing to produce music. And, additionally, will probably also attempt to have all programs that legally allow for the recording of sound also declared illegal (think Windows Sound Recorder, MusicMatch Jukebox, any program that can accept input through a stereo jack and record from the stereo jack), and programs that would convert one sound file format into another (.wav to .mp3, for example), as changing file formats may create illegal files or somehow allow copyright to be breached (couldn't changing a file format be considered some sort of reverse engineering/decompiling/other activity illegal under the DMCA?). Why don't we just declare the faculty of hearing illegal, since listening to or hearing something could be considered a way of recording it with your brain? Consumer use must be balanced against property rights before the consumer loses what remaining rights he/she has left, or we may one day find ourselves in a market where one must be legally licensed to use his or her ears.

38. *Watermarker* Says:
December 10th, 2005 at 1:02 am

[QUOTE]
Tim Thomas Says:
December 8th, 2005 at 8:11 am

As long as I have tape-monitor jacks on my home stereo amp and a stereo line-in jack on my sound card, there

will never be copy protection. "There is no security."
[END QUOTE]

That may be true for now, but don't be fooled into thinking this will always be the case. Several companies are researching audio and video watermarking which, as the name suggests, allows for a normally-undetectable code to be embedded in the digital media stream which can then be recovered at a later time by the appropriate equipment - even if the stream has been transcoded several times in either the digital or analogue domain.

There are several uses for such a technology, but here's one example: a would-be pirate goes to see a movie (perhaps shown at a digital cinema) and takes along his DV cam to record it. However, the picture and/or soundtrack of the movie has been 'watermarked' prior to playback , perhaps with information that gives detailed information about where and when the movie is being played. The pirate unknowingly catches it all on his DV cam, transcodes it on his PC into a more manageable format and distributes it on DVD or over the internet. However, the watermark remains intact despite all the various conversions between initial and final playback and so the studios are able to pinpoint exactly where and when the illicit recording was made. Or to take it further, the DV cam itself is able to recognise the watermark and, after determining that recording of such material violates copyright laws, prevents the recording from being made in the first place. Maybe even the end-user playback device prevents unauthorised reproduction. This is not science fiction. These (and similar) technologies are the subject of significant research today.

That's not to say that such technologies will become commonplace in the future but neither should you take for granted the fact that, just because all audio and video is ultimately reproduced in the anologue domain, there will always ultimately be an analogue method to copy it.

39. *Josh* Says:
December 10th, 2005 at 2:08 am

—
The same can be said for DRM. These are systems that prevent the honest from making legal use of what they have legally paid for, but that do not truly prevent illegal use. This leads me to conclude that piracy is not what DRM is about, because no DRM scheme out there today does much of anything to prevent piracy.
—

By your logic then, CD-keys are not about piracy because they do nothing to prevent it? What are CD-key's purpose then? This I want to here.

DRM is about piracy. CD-keys are about piracy. It does not have to stop 100% of piracy to be effective. If it costs $10,000 to make copy protection software (even a CD-key system) that only stops 1% of piracy in a multi-million dollar market, it's still worth it to the content producer. What other reason does the CD key exist for?

–
A CD Key does not assume you are a thief. It is closer to a key to start a car. It keeps honest people honest …
–

So you admit in your own argument that a CD-key does in fact have some effect; it keeps honest people honest? You mean it keeps people that don't have the technical know-how to download a key-gen to pirate so they give in and buy instead?

The concept of lock and key in itself assumes theft. If there were no thieves you wouldn't need to lock your doors. You wouldn't need locks or keys at all. To use your analogy in this context is illogical.

By your analogy a naked audio CD is an automobile with a push-button ignition and no locks on the doors.

Adding a limiter to the speed of your car so that it cannot go about 100mph doesn't take away your 'right' to drive, but it does impede the usage of your car. Most people would accept this because it's only when it's illegal usage.

DRM impedes your usage, but it should only impede usage that would be deemed illegal.

–
That an issue is “common” is NOT an excuse. OK, DRM will not take anyone’s life, but for Sony/BMG to secretly have software installed on people’s computers and then to find out that that software has “common” errors, that just rubs salt in the wound. It means that their programmers were unskilled. It makes one wonder — if there are *common* errors in that code, what other errors will be there that haven’t been found yet?
–

Maybe their programmers knew full well of the security issues involved with the design, told management, and it fell upon deaf ears?

Not that I would know.

40. *Josh* Says:
December 10th, 2005 at 2:10 am

~~~~

Sorry about above; wrong thread.

41. *supercat* Says:
December 10th, 2005 at 2:30 pm

The purpose of the locks on an automobile is to allow the PURCHASER of the car the means to protect his property. If the purchaser of a car wants to make 500 copies of the keys and give them to 500 people, he could do so perfectly legally. Such action may not be particularly wise, but there’s no law against it.

I do not like the ‘activation key’ business with software, and have decided against one software purchase because of it. I do use XP, which came with a couple of my computers, but if I could have gotten Win2K instead I probably would have done so.

42. *supercat* Says:
December 10th, 2005 at 2:44 pm

The pirate unknowingly catches it all on his DV cam, transcodes it on his PC into a more manageable format and distributes it on DVD or over the internet. However, the watermark remains intact despite all the various conversions between initial and final playback and so the studios are able to pinpoint exactly where and when the illicit recording was made.

What are the studios going to do with this information? I can see it as being useful in cases where media is subject to controlled distribution (e.g. when people are given evaluation DVDs for Academy-Award nominees) but not in cases where media are sold at retail (in the absense of a contract signed PRIOR TO PURCHASE, anyone who buys a CD, DVD, or other such item is free to resell it to anyone else, so even if Sony claims I bought the CD that got pirated, if I sold it in a garage sale to some unknown purchaser Sony would have no recourse against me).

Actually, I can see some legitimate uses for watermarks, but I don’t believe it’s possible to make them robust. Given three copies of a work with different watermarks, I would expect to be able to produce a composite work on which the only portions of any watermarks that would be readable with certainty would be those portions common to all three copies.

If one could produce a watermarking technology whose watermarks were undetectable without the key used to produce them, and were robuts against attacks like the above, I could see it is as being useful for a variety of purposes. Not sure it’s possible, though.
~~~~

43. *Attempting a rational thought* Says:
December 10th, 2005 at 6:46 pm

Just a few more thoughts:

1) I seem to recall that, a few years back, Sen. Orrin Hatch proposed a system by which the government could scan the hard drives of individuals for "pirated" materials, after which the materials would be deleted and the computer disabled, all of this to be done without notification, search warrants, trials, convictions. Fortunately, his proposal was not acted upon, but given what Sony's DRM programs, both MediaMax and XCP, do, and given what other DRM schemes do, it makes me wonder if private parties have decided to take his proposal to heart.

2) Saying that including a DRM scheme that installs without consumer consent on CDs is perfectly okay because game companies include DRM programs in their software is a faulty argument. Usually, the games include an EULA that notifies you that the DRM components are being installed, give you the option to decline installation (if you do so, the game fails to install), and generally do not install the DRM components if you decline the EULA. Arguing that because game companies do so is like saying that because a group of drag racers regularly race through my neighborhood without getting caught by police, it's perfectly legal to drag race anywhere, anytime, and not just drag race, but drive recklessly, drive while intoxicated, and generally break the law while driving, because others have done it. Never mind that these activites can kill and are illegal, others are doing it, so why shouldn't we?
Faulty programming aside, Sony BMG's main sin has been in the way XCP and MediaMax make it onto a user's system. Undetectable programs, incomplete EULAs, and programs that automatically install BEFORE an EULA can be read generally are considered to be legal infractions, and spyware or adware that installs under these conditions is considered illegal and the companies providing such malware can be — and are being — prosecuted. The difference between games and Sony BMG's offerings are that the game EULAs inform the user and offer a chance to decline installation, while Sony BMG hides its software, misleads the user as to what is being installed, and installs its software REGARDLESS of what the consumer decides. At the very least this is incompetence and malfeasance, at the worst this is intentionally done and illegal. You can't use the example of game companies to excuse Sony BMG's errors, they're two different examples that do not coincide.

3) To Eddie/April/Anonymous/Company Stooge:
Unlike others, I do sympathise with you. You've been hired by Sony BMG, Sony's legal arm, or perhaps an outside legal firm or PR firm contrated by Sony, to spread their views, and you have to do this job. You may even secretly agree with those of us who have pointed out Sony BMG's programming and legal flaws, but because of your job, you can't voice that allegiance.
Given your specious arguments, needless repetiton, and condescending tone of voice, however, I suspect you are firmnly in the pocket of Sony, to the point where you are ignoring customers' complaints. And this has been, and remains, Sony's MAJOR Achilles' heel throughout the XCP and MediaMax fiascos. As I'm sure you or your superiors learned in your introductory marketing class, to be successful, a company must seek out consumer input and reactions, and act on that information. Products are tailored to markets on the basis of consumer preferences and feedback, improvments in services are made based on consumer feedback, sales of a particular product can increase based on positive consumer word-of-mouth. There are even examples where, after a company has done something incredibly stupid, its willingness to LISTEN to customers and fix things BASED ON CONSUMER FEEDBACK has improved the guilty company's standing and public image. Even just seeming to listen to customers withought actually doing so can improve a company's image in the short-term.
Setting aside all legal issues, Sony BMG's main failing is that it is not listening to its customers. There is emerging evidence that at least a month before sysinternals.com publised its study of XCP, a computer repairman contacted Sony BMG about XCP. Sony and First4Internet's responses were basically to deny any problems and bury the situation. Once XCP became public, Sony and First4Internet's responses basically turned into "Tough luck, we're not going to do anything to fix the problem, if there even is a problem. You can complain and provide proof and threaten us with lawsuits as much as you want, we're not doing anything." Even the recent release of an uninstaller and pulling affected CDs from market isn't doing much to respond to the customer, since Sony has openly stated that it will stop using XCP TEMPORARILY, and is working with First4Internet on new solutions to the problem of piracy — in other words, an improved (and perhaps similarly undetectable) version of XCP, or an even more draconian new DRM scheme.
Sony BMG is taking the same attitude towards the MediaMax mess as it has to the XCP mess. Instead of

listening to its customers, Sony is ignoring them. I know some out there are going to scream "It's because of Sony's Japanese corparate culture!", but it's not. Westerners now hold positions of importance within Sony, and even pure Japanese corporate culture encourages innovation and responsiveness to customer needs — it's the same culture that gave us JIT delivery schemes, which are a perfect example of manufacturing and stocking responding to customer wants and needs by maufacturing and stocking only as much product as the consumer will buy at the moment it is needed or wanted. No, Sony BMG's attitude is simply that of the bully who rules the school playground: It can do whatever it wants and to heck with those who complain. It's this attitude that is digging Sony its grave.
So Eddie/April/Anonymous/Corporate Scrooge, start actually LISTENING and READING what Sony customers are saying and writing instead of IGNORNING it and repeating the company line. And convince your superiors that Sony needs to do the same, otherwise you'll find that no matter what you do to rectify the DRM mess, it won't improve Sony's public image. Bullies inspire fear and hatred, not love, and Sony will just inspire fervent dislike, boycotts, a perhas permanent drop in sales, lawuits, and a negative public image if it continues with its current attitudes and legal practices. So unless you and your bosses are willing to change, Eddie/April/Anonymous/Corporate Scrooge, shut up and spare us the official line.

44. *P.Dorf* Says:
December 11th, 2005 at 12:29 am

Having now been hit twice by flawed DRM software (thanks Sony!) I have started using BitTorrent. Thanks to Sony, piracy is now the safest way of obtaining music.

45. *InfoSeeker01* Says:
December 11th, 2005 at 7:07 am

Hi Ed,

Thanks for the high quality work of exposing these malpractices and unethical deeds no matter how well intend the purpose was.

Perhaps with your experience and knowledge, could you comment the followings:
1) Some thread/blog mention even an uninstallation program/technique to rid all the unwanted software (rootkit and DRM) is consider a violation of DMCA, even though the company that planted the unwanted stuff refuse to remove the software from my computer - my property.

Why a complete removal of their software is deemed a circumvention under the DMCA? Have these media companies understand the meaning of the word 'unwelcome'?

One is even permit to use reasonable force to evict a robber from one's home, why is Digital Media any different. The computer is my digital home!

2) Does it mean DMCA will not permit one to reinstall the OS to rid the DRM software? This is clearly an effective form of circumvention because once reinstalled, one could immediately turn off the autorun (bad) feature of the OS. In so doing, preventing the auto-loading of MediaMax or XCP.

I think one poster is correct. If Sony is so genuinely worried about producing something that allows unfetter copying of the IP, then they should cease to produce the good.

The way MediaMax and other budding DRM producers need to take note: Software is just 1's and 0's and doing anything thing more to prevent it from being copied is just futile. You most likely alienate your customer driving them to seek other convenient and safe way to acquire the materials.

At the moment, downloading from file share is considered safer - hence DRM producers have successfully alienated your customers. Well done for shooting your foot!

46. *MF Sprague* Says:

December 12th, 2005 at 9:18 am

Rule one when diggin yourself into a hole.. STOP DIGGING

Get some professional help (for yourself for ever considering such a thing as spyware on your consumers and for your IT organization for badly implementing/repairing/implementing/repairing/implementing/repair… such a bad thing)

47. *Anonymous* Says:
December 12th, 2005 at 3:12 pm

http://www.theregister.co.uk/2002/09/19/linux_rootkit_hacker_suspect_arrested/

so let me get this straight… it's FINE for a uk company to write a rootkit, but illegal for an individual. nice. brilliant. let's play corewars.

48. *Scott* Says:
December 14th, 2005 at 2:21 pm

"I agree completely, but as of December 6th, my local Walmart was still stocking and selling XCP infected cd's. "

XCP != MediaMax/SunnComm

Different vendor

49. *Scott* Says:
December 14th, 2005 at 2:38 pm

"The purpose of the locks on an automobile is to allow the PURCHASER of the car the means to protect his property. If the purchaser of a car wants to make 500 copies of the keys and give them to 500 people, he could do so perfectly legally. Such action may not be particularly wise, but there's no law against it."

A1) when you buy the rights to drive a car, it's called a RENTAL (sry couldn't resist). when you PURCHASE a car, it is indeed your property. however, you still cannot do with it anything that you want. ie: run your boss down with it. there are limitations on everything, be it socially imposed or morally, what-have-you.

A2) when you purchase music (or books for that matter) you are buying the *rights* to listen to, or read it. it's always been like that, whether or not you actually copied it in the 70's til now or not. the difference is that there is more advanced technology now than before. the main difference that people don't understand, is that they do not in fact wholly own the music contained on a cd. so given that premise, would you give away 500 keys to a rental car?

50. *wvhillbilly* Says:
December 15th, 2005 at 9:05 am

If music producers want to put DRM software on CDs, why can't they design it to execute directely from the CD, or install it to a RAM disk (a portion of memory formatted to act like a disk)? If they need to count copies, this could be done very simply with a registry value. This way once the disk is ejected and the computer rebooted, all traces of the DRM software will be gone, and the computer will be restored fully to its previous condition. Better yet, have the DRM software unload and the RAM disk terminate when the disk is ejected. No rootkit, no security vulnerability, no chance of corrupting the user's system, and no likelihood of conflicts from competing DRM schemes (assuming all producers use the direct execute or RAM disk schemes).

Of course, like any DRM scheme, it could be bypassed if someone wanted to go to the effort of doing so, but it seems to me this scheme would overcome a lot of the objections to the current MediaMax/XCP schemes.

By the way, I don't like DRM any better than anyone else. I think it's childish and selfish, but if we must have it, I'd rather have well behaved DRM than DRM that corrupts my system.

51. *Geoff the disgruntled* Says:
December 15th, 2005 at 10:25 am

I just acquired the CD "Thelonious Monk quartett with John Coltrane at Carnegie Hall" which is copy protected. I wanted to listen to it will surfing the Web at home on my Linux machine. Guess what? I could not do it. This is just for Windows PCs. I find this completely ridiculous. This is a reminder why I did njot buy a single CD in the last couple of years. The labels are not interested in the artists, they just want to make money out of them. If you only knew how they treat them, you'll know.

52. *Scott* Says:
December 15th, 2005 at 11:02 am

actually Geoff, i do.

i was a starving musician back in the 80's. hehe yep, the hair and everything, signed to a small label. believe me, i know. i had friends signed to geffen back then and they said in some ways, the crap i was getting dealt by our smaller label was actually a bit better in some cases than their deal.

that being said.. it's kind of easy to demonize the labels. in some cases they do it to themselves, in other cases it's really not warranted. just like MS bashing.. it seems to be fashionable, but without them, it'd be a perfect world right?

every small company aspires to be greater than it is. there is nothing wrong with that. kids get to go to college because the company makes money, right? who in their right mind is going to work for a company that doesn't make money? gotta eat, right?

MediaMax is *not* XCP… those other guys went a bad route, cut corners etc. but lumping in the industry as a whole is not fair. there *are* companies out there that really *do* care and are being hurt by this.

for example, how many actual technology companies that had new and viable tech do you think were trashed in the wake of the dot coms? that had nothing to do with the pump n dump mentality of the time? that were actually working on real technology? btw, i'm talking in a broader sense, not just about DRM.

53. *InfoSeeker01* Says:
December 17th, 2005 at 5:05 am

Hi Scott,

"A1) when you buy the rights to drive a car, it's called a RENTAL (sry couldn't resist). when you PURCHASE a car, it is indeed your property. however, you still cannot do with it anything that you want. ie: run your boss down with it. there are limitations on everything, be it socially imposed or morally, what-have-you."
You are confused with something that is a different matter. There is nothing in law to say that once you have bought a car, you could not rip off the transmission or each of the wheel to sell it or give it away.

Incidentally, DRM or even any other digital materials, you are forebidden to do this. Why? For example, if you buy an Office Professional, you are not allowed to give say Power Point to your friend because you have no need for it.

If you have bought a book, there is nothing in the law to say you cannot ripped it into each chapter and pass around to your friend the chapter you have finished reading.

If you buy a hifi system, there is nothing to say you cannot give away the speakers or the radio and keeping just one part. So why is digital materials like music and software be so different that the consumer is treated as guilty

of piracy first until he/she is proven otherwise. Why doesn't the normal law of guilt applies to digital materials.

Is it just because it is easy to reproduce? With a camera you can reproduce any scene or picture. So should camera be subjected to ban?

I am so glad to see the debate of DMCRA to put some senses back into a lopsided situation. It is time for blog like "Freedom-to-tinker" and the whole software community to rise up to correct this.

I have been through a similar era where they use laser to burn holes on floppy to discourage copying. But it is like cat chasing mouse, they even have hardware copy-card to defeat this kind of silly act. They have copy technique database released weekly like they do now with AV database.

Nothing has stopped the piracy. Borland found a good way - the Brown Paper Bag software. The software was cheap and provided support - representing good values and many users paid for it. On the other hand, they was a word processor so badly designed and so troublesome to use that no one wanted to pirate it. Even unopened sealed packets were left standing. In the end, people used them to trade for WordPerfect.

I guess you could called that the perfect software protection;-)

54. *Edward Kuns* Says:
December 19th, 2005 at 6:08 pm

Scott, you seem to be confusing the issue:

"when you PURCHASE a car, it is indeed your property. however, you still cannot do with it anything that you want. ie: run your boss down with it."

Yes, there are limitations on everything. But the kind of limitation you mention is totally unrelated to anything that DRM will do, as well as being unrelated to anything to do with copyright/patent/other "intellectual property." As others point out, once you buy a car, you are legally allowed to disassembled it and do just about anything with the parts. You cannot violate other laws, but "intellectual property" laws don't stop you from making whatever use of the car that you want. If you want to build a helicopter using your Yugo seat and engine and transmission, the FAA may complain but the Yugo manufacturers cannot.

"when you purchase music (or books for that matter) you are buying the *rights* to listen to, or read it.

100% totally wrong. What you say is what vendors want us to believe, but court cases over the past 100 years stand in direct opposition to what you are saying. When I buy a book, I own that book. I own that book in totality. It is *my* book. I am not renting it. I OWN it. I can do anything I want to do with that book. I cannot copy the content of the book and give it away. I don't own rights to make COPIES of the book, but as long as I don't make copies (other than those permitted by fair use) I can do ANYTHING I want to do with that book.

Obviously, to extend your analogy, I can't legally take a huge stack of books I have bought and push it over on someone to kill them. But as I say above, such restrictions are unrelated to "intellectual property." It's not the book distributor or the author who has the right to prevent such use — it's the government. In this context here, that makes a difference.

When I buy a music CD, I *own* that CD. I do not have the right to make copies (other than those permitted by fair use or explicitly permitted by other laws or by copyright), but I can do anything else I wish to do including give the CD away or resell it. One thing the music distributers clearly wish they could achieve is removing that right of first sale — preventing people from reselling music they do not like any more or just don't want any more. But such restrictions have no basis in copyright law.

55. *EFF: SunnComm MediaMax Security Vulnerability FAQ* Says:
January 7th, 2006 at 6:54 am

[…] What is the SunnComm MediaMax Security Vulnerability? Certain audio compact discs distributed by Sony BMG contain a version of the SunnComm MediaMax software, which creates a serious risk of a "privilege escalation attack." This new security vulnerability — different than the one reported in early November regarding Sony BMG CDs sold with software called XCP — affects all Sony BMG CDs that contain version 5 of SunnComm MediaMax software. According to Sony BMG, about six million CDs have this software. Sony BMG's list of affected CDs Is there a solution? On Tuesday December 6, Sony BMG and SunnComm made available a patch that was designed to resolve this security vulnerability. We're pleased that Sony BMG responded quickly and responsibly when we drew their attention to this serious security problem. However, the day after the patch was released, Professor Ed Felten and Alex Halderman identified a new problem. Sony BMG has now released a second patch, which security researchers are reviewing. What is a privilege escalation attack? A privilege escalation attack is the act of exploiting a security weakness in an application to gain access to resources that normally would have been protected from an application or user. This means that low-rights users can add files to a directory and overwrite the binaries installed therein, which will be then be unknowingly executed by a later user with higher level of rights. In other words, a guest user or a malicious program can effectively make changes to a computer that would normally be reserved to an administrator. Can you explain this with an analogy? Consider an office worker who has keys to her office and to the front door of the building, but not to other offices or to the supply closet. There are many ways to gain additional access: Sometimes those locks can be picked, sometimes the locks are left unlocked, and sometimes an attacker can steal the building manager's keys. This vulnerability is yet another way to gain increased access, similar to leaving the manager's keys out. By stealing the manager's keys, the office worker can escalate her privileges, i.e. get into offices and other room where she is not authorized. What are access controls? On a computer system, information resources are protected with access controls analogous to door locks. A common implementation of such access controls is called an access control list (ACL). An ACL is simply a table listing principals (e.g. user accounts) and the privileges each principal has with an object. An ACL might stipulate, for example, that user account Bob can read the spreadsheet file accounts-2005.xls, while user account Jane can both read and write it. In this example, the Bob and Jane accounts are principals, the accounts-2005.xls file is the object, and "read" and "write" are privileges. What are some details of the MediaMax vulnerability? MediaMax version 5 leaves a crucial folder "unlocked," that is to say with an ACL that allows all principals to have all privileges. The reason this is a problem is that the folder contains an executable program (MMX.EXE, the MediaMax program) that must be run by a user account with high privileges. An attacker can overwrite MMX.EXE with code of her choice, and the next time a MediaMax disc is played, her attack code will be executed. Specifically, the directory that the SunnComm MediaMax software creates, located in "c:Program FilesCommon FilesSunnComm Shared," overrides the default Access Control List (also known as the file system permissions). The SunnComm Shared directory uses an ACL that doesn't protect against low rights users (i.e., "Everyone" in Windows parlance) overwriting the contents including the installed binaries. Returning to our example of Bob and Jane, it mean that Bob can now rewrite the spreadsheet, or more worrisome, replace it with a malicious program. How could this harm consumers' computer? The SunnComm MediaMax version 5 software distributed by Sony BMG could expose the computers of millions of users to attacks by malicious hacker and virus writers. They undermine significant security protections otherwise present on computers running Windows, which are designed to prevent users (either people or programs) from gaining control of your computer. Who discovered the MediaMax security vulnerability? iSEC Partners discovered the security vulnerability after EFF requested an examination of the software, and EFF and iSEC promptly communicated it to Sony BMG. In accordance with standard information security practices, EFF and iSEC delayed public disclosure of the details of the exploit to give Sony BMG the opportunity to develop a patch. iSEC Partners' report [PDF, 237K] Who is iSEC Partners? iSEC Partners is a proven full-service security consulting firm that provides penetration testing, secure systems development, security education and software design verification. iSEC Partners' security assessments leverage their extensive knowledge of current security vulnerabilities, penetration techniques and software development best practices to enable their customers to secure their applications against ever-present threats on the Internet. Primary emphasis is placed upon helping software developers build safe, reliable code. Areas of research interest include application attack and defense, web services, operating system security, privacy, storage network security and malicious application analysis. For more information: http://www.isecpartners.com. Are there any more security issues with SunnComm's MediaMax software? We don't know. We have identified one security issue, but there may be others. Even before this vulnerability came to light, security researcher Ed Felten noted "the MediaMax software will still erode security, for reasons stemming from the basic design of the software." See Freedom to Tinker for more. We urge Sony BMG to undertake rigorous security testing on all of its software, and we will continue to look into this issue. How many CDs are affected? There are over 20 million Sony BMG

CDs with some version of the SunnComm MediaMax software. Sony BMG says that about six million have the MediaMax version 5 that is subject to this vulnerability, and has provided a list of affected titles. In addition EFF has prepared a Spotter's Guide to help you identify MediaMax CDs in the wild. Sony BMG's list of affected CDs EFF's Spotter's Guide What are some of the artists with SunnComm MediaMax CDs? MediaMax can be found on a wide variety of popular artists' music, such as Britney Spears "Hitme (Remix)" , David Gray's "Life In Slow Motion," My Morning Jacket's "Z," Santana's "All That I Am," and Sarah McLachlan's "Bloom (Remix Album)." Sony BMG's list of affected CDs EFF's list of CDs affected and possibly affected by MediaMax. Does the patch resolve all the issues with CDs with SunnComm MediaMax software? No. There are other severe problems with MediaMax discs, including: undisclosed communications with servers Sony controls whenever a consumer plays a MediaMax CD; undisclosed installation of over 18 MB of software regardless of whether the user agrees to the End User License Agreement; and failure to include an uninstaller with the CD. EFF will continue to raise these issues with Sony BMG. Does SunnComm MediaMax appear on CDs other than those released by Sony BMG? Yes. According to SunnComm, its "MediaMax technology has appeared on over 140 commercially released CD titles across more than 30 record labels." Earlier this year, SunnComm forecast "that its MediaMax CD Copy Management Technology will be Applied to More than 145,000,000 Audio CDs this Year." Currently our focus is on the Sony BMG CDs, but we are investigating whether the vulnerability exists on other labels, and urge every label that has used the MediaMax technology to check with security experts immediately. SunnComm press release: SunnComm Ups Security Another Notch SunnComm press release: SunnComm Forecasts for MediaMax Is EFF Suing Sony BMG? Yes. On November 21, EFF, along with the law firms of Green Welling, LLP, and Lerach, Coughlin, Stoia, Geller, Rudman and Robbins, LLP, filed a California class action lawsuit in Los Angeles against Sony BMG including claims arising from both XCP and SunnComm CDs. We also filed a national class action on December 2 in New York and are joined in that action by the Law Offices of Lawrence E. Feldman and Associates. Sony BMG litigation information What more does EFF want Sony BMG to do? EFF would like Sony BMG and all record labels to stop using DRM on their CDs and stop requiring its customers to agree to a EULA as a condition of playing CDs on their computers. See: The Customer is Always Wrong, DRM Skeptics View, and New York Times Op-Ed: Buy, Play, Trade, Repeat. Barring that, we would like Sony BMG to ensure, before a CD is released to the public, that it contains no security vulnerabilities, can be fully uninstalled by end users, properly protects consumer privacy including allowing consumers to opt-out of any reporting back to the company done by the CD, and is provided on terms that are fair, reasonable and fully disclosed. To the extent that they fail to do so, they need to remove such products from the market immediately, engage in a robust notice campaign and compensate consumers who have purchased them, including those harmed by XCP and MediaMax software already. […]

56. *Mediamax 3.0 and 5.0 Software Problems FAQ* Says:
January 8th, 2006 at 12:27 pm

[…] http://www.eff.org/IP/DRM/Sony-BMG/mediamaxfaq.php http://www.freedom-to-tinker.com/?p=942 […]

57. *PCWorld.com - Winners and Losers 2005* Says:
January 8th, 2006 at 3:22 pm

[…] Researchers at Information Security Partners recently identified a security flaw with SunnComm's MediaMax, an alternative copy-protection scheme found on other Sony BMG CDs. The flaw could allow a remote attacker to hijack a user's PC. This time, Sony responded with a patch almost immediately–which was quickly found to have the exact same flaw. Can you say "consumer boycott?" […]

58. *Mouse.cl: Advierten sobre nuevo fallo en parche de seguridad de Sony BMG* Says:
January 8th, 2006 at 7:05 pm

[…] Detalle de la informaciónSuscríbete Advierten sobre nuevo fallo en parche de seguridad de Sony BMGTras la polémica desatada por el 'rootkit' de Sony BMG durante noviembre, expertos en seguridad detectaron vulnerabilidades en otro software anti-copia usado por la compañía. El problema es que tras lanzar ayer un parche, tanto el sello como la EFF urgieron a los usuarios para que no lo instalen… por problemas de seguridad. 09.12.2005, 17:18 Mouse.- El parche buscaba corregir un fallo en el software de SunnComm MediaMax, incluido en 27 álbumes del sello Sony BMG, sin embargo acabó surtiendo el efecto contrario al dejar el sistema expuesto a un ataque de escalada de privilegios. Es decir, que un intruso puede realizar acciones críticas en la

computadora.Por el mismo motivo, Sony BMG y la Electronic Frontier Foundation (EFF) - una agrupación de defensa de los derechos digitales - alertaron a los usuarios para que no instalen el parche. La empresa declaró estar informando a sus clientes mediante una campaña en línea y con báneres en el reproducto de MediaMax, junto con distribuir una actualización que corrige los fallos.Pero según reporta BetaNews, el investigador de la Universidad de Princeton, Alex Halderman, ya habría descubierto una vulnerabilidad en esta segunda actualización. “Existe la posibilidad de que un intruso pueda emboscar los archivos de MediaMax para que su software hostil se ejecute de forma automática nada más instalar el nuevo parche”, explicó su colega, el profesor Edward Felten.De la misma forma, ambos descubrieron que el software vulnerable de MediaMax se instala en el PC aún cuando el usuario rechace la licencia y finalice el proceso. Peor aún, aquellos usuarios no verán el baner de Sony BMG que los advierte del fallo.”Cada disco guardado en el estante de alguien o en una tienda de música, sólo está en espera de instalar este software vulnerable en el próximo PC donde sea insertado. La única forma de lidiar con este riesgo es sacar los discos de circulación. Ha llegado la hora de que Sony BMG recoja todos los CD con MediaMax”, adviertió Felten. Hay información relacionada (haga click aquí) . Mouse Digital Email: mouse@latercera.cl / Por favor lea nuestros Términos y Condiciones de Uso. Todos los derechos reservados Consorcio Periodístico de Chile S.A. […]

59. *Digital Music News* Says:
January 9th, 2006 at 3:06 am

[…] Ed Felten Blog “MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug” […]

60. *» Anti-DRM zealots | Spyware Confidential | ZDNet.com* Says:
January 9th, 2006 at 4:56 am

[…] Freedom to Tinker has a new post today about MediaMax and SunnComm, another excellent read. The comments on Felton’s blog are interesting as well. A comment from another of Felton’s MediaMax posts: I’ll have to hand it to you Eddie and Alex, you certainly have a penchant to deride Mediamax and an obvious distaste for any kind of audio copy protection in the market place. What are your feelings on game, software and DVD copy protection? Do you feel it is your right to copy those as well? […]

61. *ITmedia?j???[?X?FEFF???□x?□?A?uSONY BMG?p?b?`?□C???X?g?[?????□??Łv* Says:
January 10th, 2006 at 1:10 am

[…] MediaMax?Z?p?p?b?`????[?X???????□œONY BMG?□?????EFF?????A?p?b?`?□닷?????w?E???□???□ł??□?P?□??B ?@?d?q?t?????e?B?A???iEFF?j?□ONY BMG?□????ńRM?i???쐸?Ú??j?Z?p?Z?L?????e?B?p?b?`?□?????????□???Ă??p?b?`????[?X???□??悤?Ăъ|?????B ?@EFF?□2??6??SONY BMG?□????????□s???A???Ђ??yCD?□g?.??▯□DRM?Z?p?uMediaMax?v?□□□??????聊?b?`????X?g?[?????邦???Ăъ|?????i12??7?????Q?□j?B ?@??????7???L?????e?B?????□G?h?E?t?F???e?????□A???b?N?X?E?z???_?[?}?????????p?b?`?□⑨??E?????B???□?□ąFF?□????□□p?b?`????X?g?[?????□??悤?Ăъ|???Ă??遂 ?@?t?F???e?????□u???O?□??ŁA?e?X?g?□??□A???p?b?`????S?ł□????□?????????Əq? Ă??遂???p?b?`????X?g?[?????Ď?s???????□s????t?g???????I?□?s???□?悤?□AMediaMax?t?@?C???□u?[?r?[?g???b?v??|???跌?@?????邆?????B ?@?.??AMediaMax?□g?p??????□??Ă????Z?p???g?.??▯□CD?□h???C?u?□}??????ŁA?U???□??g???b?v??|???烟?邦???□□邱?□???????□????B ?@?t?F???e?????□indows PC???[?U?[?□□??AMediaMax?p?b?`??킈?????□A?擺?????[?X???□MediaMax?A???C???X?g?[????킈?????□AMediaMax???g?.??▯□CD?□h???C?u?□?????□?□Ă??遂 ?@SONY BMG?□???u??I?□Z?L?????e?B?⑨?□H????邦?□v?□??āA?V????MediaMax?p?b?`????[?X?????B???炉???Ђ□??Z?p?A???C???X?g?[?????b?v?f?[?g?????B […]

62. *You Did What??? » Sony screws up again* Says:
March 13th, 2006 at 6:23 am

[…] Yeah, it’s time to stop buying Sony products. Get more of the story in Sony’s DRM security fix leaves your computer more vulnerable from BoingBoing and MediaMax Bug Found; Patch Issued; Patch Suffers from Same Bug from the Freedom to Tinker blog. […]

63. *Rich* Says:
March 26th, 2006 at 11:59 pm

Thankfully, this technology is pretty easy to defeat. In fact, if you don't have Autoplay enabled, you most likely won't be affected at all. If you do happen to have Autoplay enabled when you insert a CD, you're screwed initially, probably even more so if you accept the EULA. I did not accept the EULA, and all I had to do to remove the software was to delete the C:\Program Files\Common Files\SunnComm Shared directory, reboot, and then disable and uninstall the sbcphid driver.

More detailed instructions can be found here: http://club.cdfreaks.com/showthread.php?t=154811

64. *Abandoned Stuff by Saskboy » Blog Archive » Sony puts foot in mouth yet again* Says:
March 29th, 2006 at 12:37 am

[…] Sony started the day with its foot in its mouth. Mediamax, their other known DRM infection had a patch released a few days back. The patch opens new flaws which can endanger your computer. The EFF which is typically a good guy had sadly endorsed the patch, so now they look like idiots too. The bottom line is, don't even think about buying a CD with the Content Copy Protected logo which is a black circle with a white triangle offset in it. I tried submitting this story to fark.com as: "Microsoft files "patch with hole" patent infringement suit on Sony, after a released patch for Sunncomm DRM has a hole in it". […]

65. *DMCRA is an Ass* Says:
April 2nd, 2006 at 1:12 am

Since you can bypass Mediamax by holding down the shift key (among other ways) I guess that it's now illegal to do that. Wonder how long it's going to take some butthead lawyer to sue the keyboard manufacturers and force them to remove the shift keys…

BTW, just ripped Santana's "All That I Am" and copied the mp3s to my Moto v3i. It did take Roio about 3 minutes to "find" the audio tracks but after that it was a walk in the park.

If I were a SunnComm investor I'd be pissed because their "product" is a worthless pile of crap and once the record labels and artists figure this out the stock price is going to TANK big time! LOL!

Leave a Reply

Name

Mail (will not be published)

Website

Submit Comment

Powered by WordPress.
Entries (RSS) | Comments (RSS).

This work is licensed under a Creative Commons License.